DOI: 10.23977/acss.2024.080509
ISSN 2371-8838 Vol. 8 Num. 5

The Application of Artificial Intelligence in Network Traffic Analysis and Prediction

Shengnan Xu[a], Qianqian Wang[b]

Henan Vocational University of Science and Technology, Zhoukou, 466000, China
[a]xsnnancy@163.com, [b]wqq131111016@163.com

Keywords: Artificial Intelligence; Traffic Detection; Abnormal Behavior; Self-Learning Model

Abstract: Network security analysis plays a core position in the research field of detecting potential threats. At present, traffic analysis mainly relies on comparing behavior pattern information with predefined feature library, but this method faces the challenge of feature library structure foundation and updating lag. At the same time, due to the rapid evolution of the malicious attack strategy, it can often escape from the established detection rules, resulting in detection errors and omissions. Therefore, the intelligent security analysis system of network traffic is proposed and constructed. The system is committed to automatic learning of traffic characteristics, intelligent identification of abnormal behaviors, and in-depth analysis, which can improve the overall security and defense efficiency.

1. Introduction

The application of artificial intelligence, particularly leveraging deep learning as its core innovative force, has made a significant breakthrough in the analysis and prediction of network traffic, especially in domains like image analysis and speech recognition and this technology fully shows its in pattern recognition, future prediction and intelligent decision-making efficiency. These achievements have opened up a new perspective and solution to solve the security deployment problem in cyberspace.

2. Application background of artificial intelligence in network traffic analysis and prediction

Machine learning plays its indispensable role in many cutting-edge fields of network security, including malicious sample identification, dynamic domain name generation strategy monitoring, DNS architecture analysis, hidden channel detection, suspicious encryption traffic analysis, and deep mining of threat intelligence. The network traffic analysis technology skillfully integrates the essence of artificial intelligence and big data. Through the in-depth insight into the traffic behavior, the real-time abnormal behavior is revealed and the truth is revealed. The intelligent network management system has the ability to deeply analyze the network business traffic, and can automatically build the traffic behavior mode, and thus monitor the network dynamics in real time. In those isolated and limited professional network environments, traffic data analysis is particularly critical due to the inability to rely on the variety of abnormal detection methods of the Internet. It emphasizes the subtle insight into the traffic data, through intelligent means, extracting the typical patterns of daily traffic as a benchmark. Once any patterns departing from this benchmark are found, and it may indicate potentially abnormal behavior[1].

This paper discusses the application of the key module MI technology in the network traffic security intelligent analysis system, as well as the design and effectiveness verification of the system. Through the fine capture, efficient storage and deep analysis of real-time traffic, a set of efficient threat identification model is constructed. This innovative analysis method is embedded in the network traffic processing process, significantly improving the accurate identification and decision-making ability of potential threats and violations. With its powerful early warning function, this system can effectively reveal the threats hidden behind the long incubation period and complex attack means, and it provide powerful and timely data support for emergency response and preventive measures.

3. The application of artificial intelligence in the security field

In the current global competition of science and technology, the application of artificial intelligence in the field of security has become the key point of innovation of enterprises and research institutions. The dual correlation between technology and security: (1) technology ensures security and new technology provides energy for security, which can be used for both defensive measures and offensive strategies; (2) Meanwhile, new technology also brings new security risks, which may enhance protection and also open up a way for malicious utilization. AI's own weaknesses, if exploited, could lead to new security threats[2].

The rapid development of artificial intelligence in recent years is mainly attributed to three main drivers:

(1) New theories and technologies continue to emerge in the fields of feature representation simplification, artificial neural network, probabilistic graphical models, reinforcement learning and meta-learning, making significant progress in both academia and industry;

(2) The significant improvement of computing power enables machine learning algorithms that consume a lot of computing resources to be widely used;

(3) Massive data resources in the environment of big data greatly improve the generalization performance of machine learning models, especially deep learning technology, which allows researchers to use richer data to build effective models, further tap the potential of machines, and achieve better results in various tasks.

The application of artificial intelligence in MI security is mainly reflected in two aspects: security protection and security infringement. Security protection is the use of AI for security monitoring and protection, such as intrusion detection and defense system, and security intrusion involves the use of artificial intelligence for covert intrusion and misleading behavior, such as the attack through social engineering means[3].

4. The current application of artificial intelligence in the security field

With the innovation of network security strategy, artificial intelligence is gradually become the key to protect the network space, with its unique advantages in real-time threat identification and emergency response, as well as the potential of self learning, promote the process of network security technology innovation, artificial intelligence has widely penetrated into various security areas, show a significant practical value.

1) In the forefront of invasion prevention, the innovative technology of Israel Hexadite Company conducts intelligent threat analysis through artificial intelligence A to quickly capture and solve the

network crisis, so that the security team within the enterprise can more effectively manage potential risks. The intelligent firewall of The company, with the help of behavior analysis, can reveal the unknown threat, and protect the whole process, providing users with a strong line of defense.

2) For terminal security, Crowdstrike's terminal active defense platform relies on big data analysis, which can not only detect the secret malicious software of mobile devices, but also monitor enterprise data in real time, early warning zero-day threats, build a rapid response mechanism, and increase the cost and difficulty of hacker attacks.

3) At the security operation level, Jasper's AI algorithm assists security analysts to accurately locate potential threats in the network by efficiently processing logs and event data, which significantly improves the work efficiency of the security operation center[4].

However, despite the initial results of the application of artificial intelligence in the field of network security, its deep application is still in the initial stage. In addition to improving the protection performance of some products, the establishment of a comprehensive safety protection system based on artificial intelligence is still in the experimental and exploration stage. Foreign companies, such as DmkTiace in the UK, have applied machine learning and artificial intelligence technology from Cambridge University to the bionic immune system, aiming to realize the automatic protection of the network and effectively combat artificial and machine learning-driven attacks. In contrast, the domestic development in this aspect still needs to be strengthened, and it is urgent to study how to integrate AI technology into the overall architecture of network security to achieve innovation and optimization.

5. The application of artificial Intelligence in the intelligent analysis of network traffic

As a crucial data, network traffic carries rich information about network and user activities, and covers almost all network-related events. From the perspective of network security, network traffic characteristics play a key role, because these features are often accompanied by when hacking or other threatening activities occur. For the network infringement, no matter whether the attack succeeded or not, its behavior must be reflected through the network traffic. Therefore, by collecting and analyzing large-scale network traffic data and using intelligent system model, it can automatically detect abnormal patterns and unusual activities in traffic, and immediately issue alarms. This helps to identify unauthorized application protocols and cyberattacks, and increases the speed and efficiency of users' response to application exceptions.

5.1 System functional architecture

In-depth analysis of the dynamic data characteristics of abnormal behavior and network attacks, its potential in improving the advanced detection of network traffic can not be ignored, can effectively break the current technical limitations, and significantly improve the insight and early warning response to new threats. According to the operation steps, the intelligent network security management system first receives and processes the collected massive information, and then screens out the key data, and uses the intelligent analysis module for in-depth analysis. Ultimately, the system can accurately identify abnormal behaviors, monitor potential threats in real time, and support the fine management of data sharing strategies. The functional architecture of the system is shown in Figure 1.

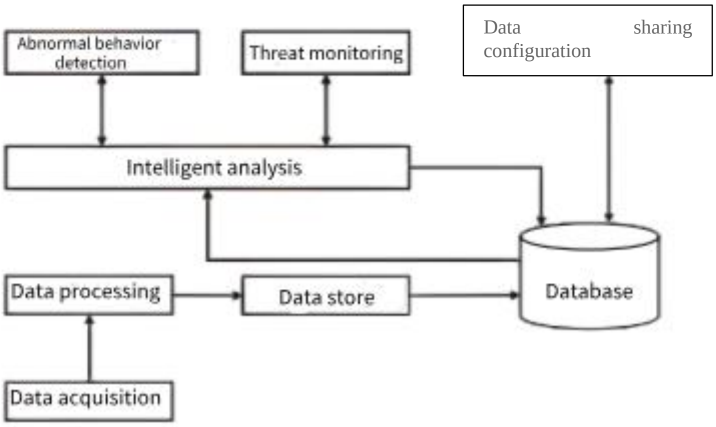

Figure 1: Functional Architecture

1) The traffic monitoring unit receives the real-time data flow transmitted by the probe to ensure the comprehensive network traffic acquisition. Data preprocessing units perform key steps such as normalization and normalization to ensure consistency and availability of data.

2) As the core intelligent tool set of the system, the intelligent analysis module includes a variety of analysis means, such as correlation analysis, search insight, deep learning, behavior analysis, artificial intelligence-driven analysis and visual model construction, aiming to provide deep-level analysis strategies.

3) Abnormal behavior detection module to explore all kinds of abnormal behavior pattern, build precision abnormal behavior identification model, effectively identify the network violations, covering a wide range, such as data breach warning, account intrusion detection, outlier analysis, long-distance VPN activity monitoring, compliance audit, abnormal login behavior tracking and authority abuse and assets external monitoring, etc.

4) The security threat identification module provides insight into the potential risks of the network through advanced intelligent analysis of full traffic data. Various analysis strategies such as single data characteristics, periodicity and frequency are used to identify threats, such as external connection attacks, abnormal traffic patterns, violent cracking behaviors, and even SQL injection. In addition, the module has the ability of adaptive learning, can dynamically adjust the model parameters and thresholds, and distinguish the traffic type and application layer attacks.

5) The data sharing and configuration management module plays the role of the coordinator, receiving policy instructions from the management system, and is responsible for software configuration, status monitoring and information reporting. In order to promote data exchange and sharing across systems, the module establishes strict data sharing specifications, unified interface standards, parameter settings and communication protocols, and ensures the seamless flow of traffic data between multiple systems.

5.2 System software architecture

In the design, the software functions are finely divided into five key modules: data acquisition unit, data import link, storage and operation layer, intelligent data analysis module, and security application. The data acquisition module continuously captures the comprehensive flow information in real time through the efficient probe, and adopts advanced algorithms to identify the traffic characteristics in real time. The acquired data is seamlessly connected to the data import layer through standardized data access channels, which is responsible for the preliminary data collation, warehousing, and strict management and monitoring of the data source.

The storage and computing layer builds a distributed data processing platform, with the ability of dynamic resource scheduling. The intelligent data analysis module covers a variety of analysis functions, including quick retrieval, in-depth insight and behavior mode mining, etc. Intelligent security analysis based on intelligent model can perform complex tasks such as correlation analysis, in-depth analysis and behavior pattern prediction, and conduct centralized management and intelligent optimization of model execution.

5.3 System key and health technology

The traffic self-learning scan of the network baseline is designed to identify the regular network condition, among which the most critical is to set the learning architecture. This architecture defines learning methods and application rules, involving parameters such as the length of learning periods, the number of learning iterations, the way scanning strategies are formulated, and the conditions that trigger automatic scanning. Traditional detection methods often respond against such latent threats. The detection technology for this invisible malicious traffic relies on the long-term flow mode analysis, and identifies the hidden malicious activities that artificially reduce the frequency through the horizontal and vertical comparison of behavior characteristics. The behavior sequence modeling based on hidden Markov model is used: 1) extract the behavior characteristics of the current user from the network traffic data; 2) obtain the behavior characteristics from the training sequence, establish normal sequence library and train the state set of Markov chain to calculate the state transition probability matrix to describe the normal behavior pattern of the user; 3) compare the behavior characteristics of the current user with the historical behavior, if the difference exceeds the preset threshold, abnormal behavior; otherwise, if the difference is within the normal range.

6. Demonstrate the validation environment

In order to comprehensively evaluate the performance of the network traffic security intelligent analysis system, including its ability of data capture, storage, in-depth analysis, intelligent threat intelligent identification and real-time abnormal traffic monitoring, a set of rigorous functional verification and real scenario simulation test are designed. The system is installed in the key entrance and exit of the enterprise internal network in the actual combat verification stage. During the demonstration and validation phase, the system's most streamlined deployment configuration is used to highlight its core functions and response efficiency, as shown in Figure 2.

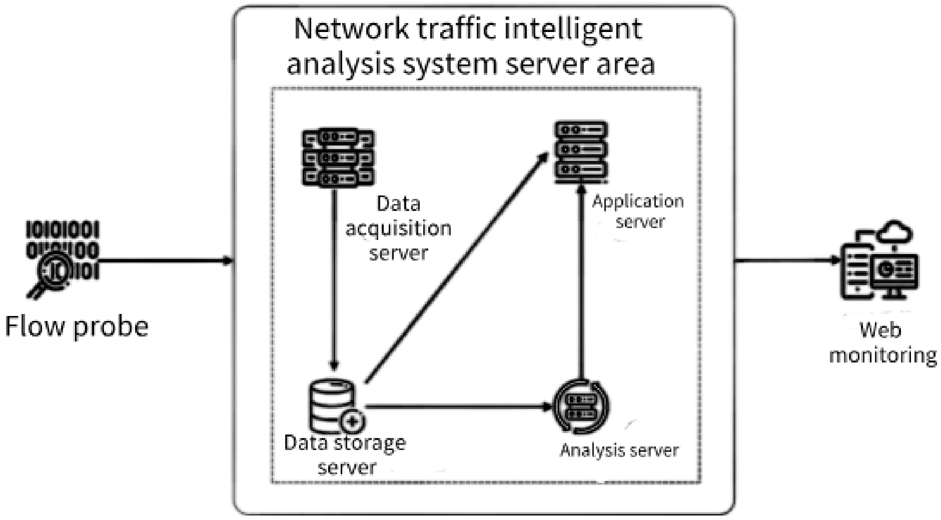

Figure 2: Network traffic security intelligent analysis system demonstration and verification deployment

6.1 System analysis model

This paper aims to discuss how to design customized security architecture according to network characteristics, and deeply study the application of data mining model in the field of network security, integrating general intelligent processing strategy and cutting-edge threat identification technology, to build a unique set of network traffic security intelligent analysis system. The core of this system is to establish a data analysis model closely linked to practical application scenarios, clarify its implementation path, and elucidate the key role of intelligent components, including but not limited to the selection and integration of intelligent algorithms[5].

6.2 Verification of key indicators

In the experimental environment, the following four core aspects can be evaluated for the characteristics of the network traffic security intelligent analysis system:

1) The system shall have the intelligent analysis ability of network traffic, and build a traffic behavior model according to the network service dynamics, so as to detect the abnormal traffic in the network in real time. In a specific independent or closed network environment, we cannot rely on Internet tools to detect internal anomalies, so the intelligent analysis of traffic data is crucial. By analyzing traffic patterns through intelligent technology, once the flow deviates from this benchmark, it may indicate abnormal activity.

2) The attributes of supported machine learning algorithms should cover seven key dimensions, including application protocol category, source target address, number of data packets, byte number distribution, traffic direction, time factor and data type. Abnormal behavior may appear in multiple levels of traffic characteristics, such as illegal protocol use, abnormal traffic magnitude, time series errors, etc. Therefore, the required machine learning algorithms should be able to handle these underlying traffic properties.

3) The analysis model should have the function of self-learning, which can dynamically adjust and optimize the parameters and thresholds, and effectively identify the traffic attacks and the application layer attacks. In the actual operation, the normal flow standard will change due to the business stage, time, region and system differences, so the flow analysis model needs to have dynamic adaptability.

4) The data feature modeling methods of network behavior should cover more than five ways. Abnormal network behavior has specific landmarks, and the identification model relies on data features for matching analysis. At least it should be able to identify five types of abnormal behavior, including illegal accounts and improper permissions.

5) The system shall be able to identify more than four kinds of network traffic attacks. The characteristics of cyber attacks will appear in the traffic data, and it is crucial to identify no less than four typical attacks [6]

7. Conclusion

To sum up, to carry out the application research of artificial intelligence in network traffic analysis and prediction, the core function of the innovative network security intelligent monitoring system built in this study is to efficiently identify potential threats and accurately track the source, providing indispensable data support for rapid response and early warning. The design is to realize the intelligent upgrade of traffic analysis, through the construction of intelligent network traffic security analysis model, systematically analyze the abnormal dynamics in the explicit data flow, automatic alarm abnormal traffic and unusual behavior, at the same time, can identify the malicious application protocol and network infringement behavior, showing a strong real-time protection ability.

References

[1] Xiao Junbi, Wei Jiaojiao. Review of network traffic analysis and prediction research for data mining [J]. Computer and Digital Engineering, 2023, 51 (02): 372-379 + 467.
[2] Guo Shuanqi. Modeling and predictive analysis of massive network traffic with big data analysis technology [J]. Information Technology, 2021, (04): 102-106 + 112.
[3] Li Gang. Cluster analysis and wireless network traffic prediction of neural networks [J]. Modern Electronic Technology, 2021, 44 (07): 91-94.
[4] Li Xiaohui, Chen Chaoyang, Yi Huawei, Li Bo. Large-scale network traffic prediction based on cloud computing and big data analysis [J]. Journal of Jilin University (Engineering Edition), 2021, 51 (03): 1034-1039.
[5] Xu Huixiang, Cao Min, Ma Yingying. A combined prediction model for nonlinear network traffic based on big data analysis [J]. Journal of Shenyang University of Technology, 2020, 42 (06): 670-675.
[6] Tang Zhoujin, Peng Tao, Wang Wenbo. A local least-squares traffic prediction algorithm for small-scale network based on correlation analysis [J]. Journal of Physics, 2014, 63 (13): 57-66.